

疫情防控下的大数据价值 与隐私伦理问题研究

易书凡

(南京师范大学 公共管理学院, 江苏 南京 210046)

[摘要] 相关大数据技术的应用为疫情防控与治理提供了高效和扎实的技术基础,在重大疫情治理和防控的过程中,大数据技术既为疫情防控提供了高效性,减少人力资源的损耗,也使疫情防控更具有精确性,准确定位了疫情相关人群,既提高了诊断的准确性,也为医疗人员提供了更多知情和防范可能,更加保障了医疗人员的安全,大数据对个人的安全程度进行识别,比如健康码的使用,也对疫情治理下甄别提供了准确性,为之后的经济复苏提供效率。大数据技术的使用原理是对个人数据的挖掘与使用,对个人隐私的侵犯存在不可躲避的可能。个人的隐私含义犹如一只变色龙,含义随着环境的改变而发生变动。尤其是在我国对隐私权的法律建设明显不足,隐私权并未作为一项单独的权利被保护,总是依附于各种其他的权利之中,这使得大数据下的个人隐私危机愈加凸显。文章从伦理角度补充对个人隐私的保护,站在疫情防控社会安全和个人隐私角度的辩证立场,提出大数据技术下个人隐私伦理建设的具体路径。

[关键词] 疫情防控; 大数据技术; 隐私危机; 隐私伦理

[中图分类号] B82-057 **[文献标志码]** A **[文章编号]** 2095-0292(2020)06-0045-07

一、疫情防控下的大数据技术价值

习近平总书记发出号召:“坚决把疫情扩散蔓延势头遏制住,坚决打赢疫情防控的人民战争、总体战、阻击战。”这份号召对于疫情防控作出的要求就是要从全局出发,要有着高效率的工作能力,这与大数据技术的属性不谋而合。大数据技术对数据收集有着总体的要求,对数据的收集的技术原理就是大量全局的数据,强调数据的全样本、相关性和预测性,信息的丰富将符合全局的视野,准确预测和人力节省也为疫情防控提供着“高效”,大数据技术的应用将成为这次疫情的防控和治理不可或缺的技术支持。

(一) 提升医疗水平,保障医务人员安全

决胜疫情的关键因素就在于医疗救治的水平,即有关于疫苗的开发、感染患者的治疗技术。基于信息时代对于互联网的成熟利用,医疗数据可以即时地分享到各个区域的医疗团队,使得各救助集团可以第一时间得到与疫情相关的宝贵医疗数据,这些被共享的数据是制订治疗方

案、研发疫苗的基础。而大数据技术可以广泛收集这些资料,通过系统化的数据分析,进一步提升诊断方向和诊断预测的准确性。

在信息时代背景下,大数据技术成为提升医疗信息化水平的技术支撑。其一,大数据技术有助于线上疫情治疗工作的开展,帮助线上资源的整合和线上平台的搭建。对于疫情的在线诊断和治疗,大数据可以共享这些数据,实现联防联控、群治群控。线上疫情治疗工作的展开减少了现实医院的拥挤和大量的人口流动,避免引发交叉感染,也使得在家隔离的人群更好地对自身情况了解和反应,这种做法不仅降低了人群被感染的风险,还缓解了有限的医疗资源与无限的医疗需要的压力,可以将医疗资源用在刀刃上,更多地阻击疫情恶化与蔓延。其二,对于线下治疗手段而言,大数据同样拥有着独特的作用,对每位线下患者的身体数据进行数据监测,可以及时进行治疗的跟进,对数据进行建模也可以优化诊断流程,对群体医疗数据的智能分配,还有利于整体疫情治理工作,防止出现一时的资源短缺状

[收稿日期] 2020-09-26

[作者简介] 易书凡,南京师范大学公共管理学院伦理学专业硕士研究生,研究方向:应用伦理学和经济伦理学。

况。

大数据技术基于对数据的收集,进而进行数据分析和预测,这就是大数据技术中人工智能的运用。利用人工智能诊断疾病不仅可以大大提升诊断的准确率、缓解医务人员不足的窘境,还能最大限度地预防和降低医患之间交叉感染的风险。如何应对“人传人”的病毒传播不仅是防治新型冠状病毒肺炎这一重大疫情的难点,还是保障医务人员生命健康的关键^[1](P32-41)]。大数据在医疗中的应用有力地支持各种防疫手段和办法,也更好地保障了医务人员的安全。

(二) 疫情防控效率提升

首先,由于疫情需要及时有效地遏制扩散,在防控时必须投入大量的人力和财力去排查疑似的病例。新冠病毒的高传染性、全国人数众多、交通活动状况极其复杂等难点对全国医护人员劳力的考验是相当艰巨的,有限的医护人员要想在短时间内排查传染源和密切接触者,进行人力上的亲身彻查,不仅防控效率不够,而且这对医护人员的工作环境也充满了疫情的威胁。在疫情的防控阶段,是最需要效率的阶段,仅靠人力的摸点排查无疑是对疫情关键节点的防控具有破坏性的,大数据技术的效率价值就此凸显,效率使人民能够及时地站在疫情防控的最佳时机和节点,使疫情防控工作拥有更多的时间和人力。

大数据对于新冠肺炎疫情的防控效率价值主要体现在对个人信息数据的有效采集,可以及时控制传染源和切断传播途径。在对疑似病例的排查时,大数据对信息处理有着全面整合的技术特点,对全国铁路、公路、航空等交通信息可以进行高速有效的排查,再通过健康码的方式可以迅速识别个人的安全状况。通过对疑似病例相关活动信息的收集可以摸查其接触人群,相较于个人的回想和说明,这种信息收集方式排查接触人群才更显得可靠,由于新冠病毒具有的高传染性,在人员排查上要排除主观的判断,用客观信息说话,做到对人民的健康负责。

(三) 疫情布控数据化的科学性

在监控疫情时,科学合理地出现疫情状况的区域进行布控工作,是扭转并维持转好事态的关键点。在隔离好相关确诊病例、检测好相关接触人员的同时,我们也需要关注好新冠肺炎疫情的传播方式,在对人员加强管理的同时,也应关注好对地方区域和设施的布控。大数据技术可以采集全面的数据并利用相关的技术进行预测和分析,建立在事实数据层面的布控,更加全面科学地利用大数据技术布控,从一定角度来说与我国的国情是相符合的,由于我国人员密集广泛的流动,只有使用大数据技术进行科学布控,才可以更有效地遏制疫情蔓延,在产业经济恢复上更具效率,盘活了疫情防控,生活保障和经济恢复之

间矛盾的关系。

对于决策层面,基于大数据分析的精准预测,有助于相关部门对区域的部署科学决策,对政府部门的布控决策起到助力作用,降低了主观的判断影响,使得疫情布控更加从数据事实层面出发,科学合理布控。大数据技术带来对疫情状况数据的精确预测,可以对各区域的人员活动进行明细统计,对未来的疫情状况进行精准判断,使得政府对医疗资源、人力资源等其他资源的分配合理有效。在关联技术使用层面,大数据技术支持人脸识别、口罩识别、红外感应、热成像测温、无人机警示等。大数据技术衍生的相关应用,对于区域布控来说就像是更多的棋子,对于疫情防控部署也有着更多的手段提升布控效果,不仅对人流活动密集的区域实现了有效防控,还实现了更安全的监测预警模式,做到对疫情防控、生活保障和经济恢复之间的“三不误”。

(四) 优化升级防疫体系

大数据技术曾应用于2009年暴发的甲型H1N1流感疫情中,谷歌公司就对庞杂的网络检索词条进行大数据模型分析,其预测结论与最终官方数据相关性高达97%。大数据让预测疫情成为可能。除此之外,大数据价值还在于为优化完善疫情治理制度和系统提供重要保障。新冠肺炎疫情的防控体系必须是一个先进完整的系统,对管理模式、基础设施以及科学技术等方面要求应用全面合理效率。大数据不仅为优化防疫体系的全面升级提供了技术支撑,还在大数据人工智能方面为管理模式、思维理念提供决策建议。

体系防御疫情的主旨在于对疫情状况的快速反应和制度治理,对扩大疫情战果、预防疾病传播,保障生活秩序、维护社会安定起到了重要作用。自2003年“非典”疫情之后,对于体系防御疫情的问题,我国提出了“建立健全疾病预防控制体系”的目标,各部委出台了《关于疾病预防控制体系建设的若干规定》等规范性文件,这份文件对我国防御疫情体系提出完善和修整。而大数据技术提供了庞大的疫情数据进行收集和处理信息的可能,这使得疫情在大数据的预测下变得更好控制,使得政府可以有针对性地建立防御体系,优化防疫体系。

在疫情治理工作中,人工收集汇总上报的情报难免会有疏漏或者是应对不及时的问题。利用大数据的技术采集形式,让整个疫情的数据流汇总在一起,用客观科学的技术分析建立防疫体系,不仅使得防疫工作更加细致,还可以通过数据预测的方式对疫情主动提前布置策略,让防疫体系难有疏漏,更富有主动性。

二、大数据技术下的隐私伦理危机及其根源

随着大数据技术在疫情治理中发挥着不可替

代的价值,大数据时代隐私保护伦理问题也渐渐浮出水面,问题本质就是两对范畴即矛盾双方大数据技术利益与人格尊严价值冲突的结果。大数据技术造成隐私伦理危机,即技术在带来社会效益的同时,导致个人的隐私数据不再受自我控制,甚至个人的隐私数据走向交易市场,这些隐私数据在个人不被允许甚至不知情的情况下进行二次交易,这对个人的安全生活构成侵害和隐患。通过对个人大量隐私数据的采集,对个人的行为进行数据预测,不仅会伤害个人的名誉权,还影响了个人自我选择独立思考的权利。

我们找寻参与的主体即大数据技术本身和政府法规以及参与个人进行考量,就能得出隐私伦理危机产生的根源。

(一) 技术根源: 大数据技术存在逻辑缺陷

大数据技术的使用逻辑是建立在互联网搜集不断产生、传播和存储的数据。数据的广泛搜集与个人隐私的要求充斥着本质的不可调和的矛盾。由于技术使用本身的特征和属性,无法通过升级技术本身实现,而是需要从内部解决其自身存在的逻辑缺陷。

大数据技术应用的过程就是通过对海量数据的分析,然后建立大量数据的预测指导我们的决策与生产。数据的使用从头到尾都充斥着隐私泄露的风险,数据挖掘是大数据能够使用的前提,个人普通的具有单一属性的数据,通过大数据技术的梳理、整合、分析,往往对个人的隐私具有深刻的威胁。信息生产者是否拥有其生产者的信息控制权,将是判断隐私是否被侵害的标准。即使每一次信息使用都建立在信息生产者的许可之上,由于数据挖掘的深入,隐私信息的流出是必然会发生,因为大数据技术广泛而深入的数据挖掘使用时无法避免每一个有可能出现的漏洞。大数据技术的发展不仅仅是为了社会经济的发展,对于满足国家安全和军事的需要也充当着重要角色,此时个人利益和国家公共安全的利益就存在不可避免的冲突,需要在伦理的层面提出适合的做法。

大数据技术来源于互联网空间的联通与共享,共享虽然有相当的益处,但其背后的风险也是随之而来的。现在互联网信息共享缺少明确的制度指导和法律保护,一味地进行共享信息的行为只会导致各种信息泄露频发,进而威胁国家安全。互联网数据隐私政策目前仍然只是在初步实践阶段,不适合大规模实现应用。共享的技术特性所带来的隐私伦理问题的技术性根源问题,这种网络空间所带来的问题,技术跟不上,也无法通过人工的补救来解决,这是技术发展中间阶段时必然会发生的问题,更重要的是我们要在发展技术的同时,谨遵技术发展真正的要义和价值观。

(二) 制度根源: 法律适用社会发展的滞后性和伦理规范缺失

人类社会的发展并不是一个匀速的进程,是呈现出一个加速发展的曲线,必然会导致发展之间的不协调,正如经济发展是基础,网络技术带动了经济发展,必然会导致上层建筑法制建设的跟进不及时,这并不是指我国法制的问题,而是指这种具有先后逻辑性的条件,必然会呈现的一种特殊时期的法律滞后导致的法律规约漏洞。我国对网络隐私权的具体保护条款主要以两种方式应用:一是参照上位法间接地保护网络隐私权;二是通过一些明示性表述的法律条款针对情况进行保护。“虽然我国越来越重视隐私权的立法保护,但是有关网络隐私权的法律条文与西方国家相比仍然较少,并且随着互联网的迅猛发展,网络隐私侵权频发,部分隐私权法律法规尚不足以应对网络空间的新情况,健全网络隐私权法律法规,充分保障每一位自然人的人格权,加大网络隐私侵权的惩罚力度,才能营造一个更加安全可靠的网络空间”^[2](P36-38)]。

隐私伦理失范的根源之一就是互联网环境下缺乏隐私伦理原则的指导和相关法律法规跟进滞后。原本建立在现实社会中的法律规约、道德规范等制约体系,因为环境的改变,个人隐私范围的变化,线上不能与线下同步,很多法律法规形同虚设。在线下的传统活动的领域,因为常年的管理经验和监管经验,市场的管理与监督机制在运行中逐渐适应市场,而现有的管理规范与监督机制并不能及时适应新的网络技术环境,适用网络环境新的道德规范和法律法规还没有建立得很完善。大数据技术在采集个人隐私信息时不受现实法律、道德规范的制约,这种发展进程的法规和道德规范的滞后问题使得大数据技术的应用毫无约束。

法律法规和道德规范的滞后性体现在对大数据技术应用的监管力度较弱。虽然法律规范和伦理原则并不等同,但当大数据技术应用在社会中,总是会依据法律所要求和允许做的事情的范围内活动。法律既为社会规范提供了非常重要的指导,也为伦理准则提供了支持。目前,我国的立法存在许多不足,只有一些相关的法律中涉及这一问题。比如,《计算机信息网络国际联网管理暂行规定实施办法》第18条规定“不得在网络上散发恶意信息,冒用他人名义发出信息,侵犯他人隐私权。”2000年11月发布施行的《互联网电子公告服务管理规定》对个人信息保护的规定如下:“电子公告服务提供者应当对上网用户的个人信息保密,未经上网用户同意,不得向他人泄露。”2015年,《中华人民共和国广告法》第二章第九条规定“广告中不得出现危害人身、财产安全、泄露个人隐私的情形。”从

上述可以看出，隐私权立法并没有放在独立权利类型的地位。因为网络技术起步较晚，相较于国外相对长时间的法律体系完善，我国关于隐私方面的法律保护缺乏时间积累。对于大数据应用正一步一步走向完善的发展，现有的法律需要及时地更新来面对更加复杂的隐私保护的状况。对于大数据技术的应用，法律对于边界行为的规范是必不可少的，互联网空间下的活动只有在良好的法律基础下才能可持续发展，才能构成长久繁荣。大数据技术使得信息传播的速度无法想象，个人隐私问题将越来越难以控制，法律建设必须随时跟进，从而减少不良道德行为的发生。

由于缺乏相应法律的支持，伦理道德的规范具有局限性，导致对大数据技术的约束力减弱。大数据技术应用中隐私伦理失范行为的大量发生在很大程度上是因为互联网隐私伦理的道德规范体系的不完善。一个正常互联网空间如果缺乏必要的伦理道德规范。线下的道德规范与线上的道德伦理规范如果存在冲突，在网络空间中人们的行为就会失去正确的向导，造成行为的失范。对于互联网的大数据技术，现在的法律规定往往是僵硬的、边界模糊的，在法律无法涉及的领域，伦理道德规范的必要性就体现出来。虽然互联网已经普遍应用到社会各个行业，但缺乏系统的道德规范。只有一些伦理协会和商业监督组织制定了一些协会性和行业性的网络道德规范，诚然，这些规范无疑对人们的行为规范起到一定积极作用，但利益驱动行为仍然会逾越道德的边界，因此才产生了如此之多的不良行为，只有整个社会都有认同的具体的伦理原则，既有企业的自发，也有全社会的监督，市场才能发展得更道德和可持续。传统的伦理道德规范是在传统社会的发展需要下应运而生的，虽然起到一定的作用，但面对网络道德规范，在网络社会的发展下，对于伦理道德规范会不断出现新的内涵和要求。网络环境的虚拟性在很大程度上让人放松了平时生活的规范要求，这样一来，会使人弱化网络环境中的道德规范。网络环境的伦理道德建设，还存在许多值得思考和解决的问题，对于引导互联网营销的方向，伦理道德又起到指示牌的作用。只有遵守了例如互联网营销中的隐私伦理原则等众多伦理规范，互联网网空间的经济生活才能真正地服务于群众。

（三）意识根源：各主体的道德伦理意识尚未形成。

分析互联网发展的历史，各主体道德伦理意识的缺乏都是伦理问题产生的重要原因之一。虽然一定时间、空间内的伦理道德要求会有所不同，但履行道德义务尊重个人隐私是始终应该坚持的态度。

时下，由于大数据产业的资本化进程的进

行，整个社会经济发展的运行越来越依赖个人的伦理道德意识，提高各主体的道德伦理意识能够有效地减少因为个人道德认知不充分、社会责任感缺乏而发生犯下侵犯他人财产与信息安全的行为。人是实践伦理规范的主体，任何理解世界、改变世界的行为都必须以人是主体作为基本前提条件。处在互联网空间的主体都弱化了其作为主体而存在的方式，即带来了个主题道德意识淡薄，因为感到“自己不是自己”。这种弱化的具体表现有四个：一是匿名性，很多具有隐私意识的网络使用者在网上发表的言论默认是具有匿名属性的，从而无法对应真实身份，而且平台也创造了无须公开的条件，虽然随着时代的发展，我国互联网空间涉及公共领域负责的部分都是要求对应真实身份的，但显然大部分情况下，你的真实身份并不影响你在网络上发言交流沟通情感的权利，这也使得个人的行为脱离主体的道德感。二是网络空间人际平等带来的去中心化，即信息的传播都是双向的、分享的，并无领导核心这种高人一等的网络内的组织控制，这种去中心化给网络空间带来了网络活动的高效率性、高沟通性，这也带来了一旦有失伦理规范的行为，影响的广度和速度都是巨大的，伦理失范的破坏性巨大，这种平权效应弱化了互联网空间内人的伦理道德树立。三是中立性，这里中立性是人为管制的价值趋向和结果，网络空间内要求的多元化发展导致偏向各个价值观的中立，这对于强调主流意识的道德伦理规范是不利的。四是互联性带来了网络空间信息的高扩散性，网络空间不再像真实世界需要各式各样的载体去完成信息的传播，网络空间构成的本身立场就是互联的信息，所以整个世界的互联网构成了一个整体，这种无限制的传播虽然是高效的表现，但是在种影响下对伦理规范的意识培养就显得尤为重要，需要坚决树立伦理的方向标，防止可能潜在伦理失范造成巨大的破坏和影响。

我国虽然互联网发展迅速，成效颇多，但是缺乏系统的网络道德教育普及。综合来看，我国网络道德教育是一块短板所，抓住短板，重视网络道德教育作为防止隐私伦理侵犯的手段将是事半功倍、具有效率与智慧的方法。

三、大数据技术下的隐私保护的伦理对策

上文对于大数据时代隐私保护伦理问题的根源分析，可以有针对性地得出大数据技术下的隐私伦理保护的对策，建立一套适应各主体参与的大数据技术发展的伦理准则，帮助各参与方将道德规范内化为自身的行为方式，并通过监督约束机制与伦理准则相辅相成。

（一）提出遵循大数据技术下的隐私保护伦

理准则

在互联网营销的背景中，想要构建隐私的伦理原则的出发点是以各主体的责任为落脚点。在大数据时代隐私保护伦理准则的构建中，围绕“责任”的主题，赋予各主体伦理准则新的内涵，使其更多地关注个体科技行为带来的后果与各参与主体的责任，这样的伦理准则既切合技术也顺应社会。

1. 企业主体：企业利益与社会责任并重

诚然，企业的营收决定了自身的发展与生存，但无视社会责任以及忽视消费者权益的运作方式无疑是杀鸡取卵，无法可持续的发展行为，为了短暂的一些利益而忽视企业自身的社会责任实则是盲目的。企业社会责任指的是高于自身营收目标的社会义务，这种社会义务看似与营收是矛盾的，但其实更有利于整个市场环境与企业长远发展。在互联网营销中的主要商业主体企业应当遵循社会主义下的商业伦理准则，关于隐私伦理的就是：企业在商业活动中应当尊重个人包含尊严和自由的隐私权力，企业主体通过多方商业领域的参考，从而进行明智的决策。

在互联网技术应用日益发达和成熟的今天，成熟的互联网企业拥有了信息使用的主动权。跟随主动权的视角会发现行业自律显然也必须是保护隐私的重要举措。例如，美国政府在促进发展互联网营销和互联网技术应用的同时，一是以法律维度为支撑的保底保障，二是提出了建设性行业指导、网络隐私认证计划、技术保护、行业内自律规范等四个方面行业自律方式。这四种方法对于我国企业的行业自律提供了良好的借鉴性的参照模式。

虽然我国的互联网发展看起来是相当成功的，技术应用得越来越快，隐私侵犯问题却愈加增多。类似于《互联网搜索引擎服务自律公约》和《互联网终端安全服务自律公约》等公约的发布，内容围绕保护、保障用户个人数据安全和个人数据的使用知情权，设置了相关条款。政府对于隐私伦理建设作出许多相关行业自律的尝试，未来隐私伦理的建设完善充满着可能性。

互联网企业利用大数据技术创造利润和营收是不可避免的资本驱动行为，但如何创新和发挥互联网技术来造福群众才是真正目的。工信部于2016年伊始就正式印发了《大数据产业发展规划（2016—2020年）》。大数据技术发展不止于产业竞争力，政府更指出了要发现和全面提升大数据技术的优势，对大数据的五年发展进程进行了具体的部署。该规划的发布在肯定大数据效益价值的同时，兼顾个人隐私的保护，对于个人信息的使用做好保护和监管。行业自律不仅在其自身，政府还必须建立健全对企业的监管制度，对隐私侵犯行为实施严厉惩罚。不仅是通过监督

的方式，还要教育并指导行业内部的自律意识和产权保护意识的发展，企业应设置数据保护的专职部门对隐私保护进行评估，科学分析、推测大数据技术应用中可能存在的隐私泄露风险，这都是政府为了帮助行业自律提出的具体方法。

大数据技术必须遵守技术条款与伦理规则。随着欧美国家针对技术创新领域的伦理建设进程，“负责任创新”被提出而且受到理论界和社会广泛的重视。“负责任创新”这一理论是可持续发展的重要组成部分，比如在大数据应用上通过分析利益相关者全体，提升大数据技术应用的全面效果。考虑到大数据技术应用在自然和社会环境中造成的后果以及所面临范围的影响和涉及社会需求和道德价值的结果和选择，正确评估两对范畴之间的关系，为新的研究、产品和服务的设计和开发的功能性提供方向。

总之，在构建互联网营销中隐私保护的伦理原则时，我们要秉持企业利益与社会责任并举的理念，在发展互联网营销时始终遵守这种可持续发展的并举原则，在技术创新的同时，注重对大数据技术的创新和设计过程进行全面的综合考量与评估，技术创新要充分调查用户的真实需求，将技术带来的利益与责任相结合，只有大数据技术坚守这种伦理原则，尊重个人的隐私，其本身才可以良性发展。

2. 政府主体：自由与监管适度原则

构建政府主体的伦理原则理论就是考虑监管与被监管之间的辩证关系，在寻找二者关系之前首先要看懂相关范畴含义，需要知道自由是人之为人本身最基本的需求，是人性内在价值和达成自我实现与社会进步根本条件的外在价值的综合体现^{[3] (P1005-1007)}。互联网空间中的个人，由于互联网的特性以及倾向需要的技术调整使得人在互联网空间中的自由难以真正为自我所控制。个人不得不牺牲某些程度上的自由去换取行业或是环境安全的需要，当今社会的数据化进程也逐渐加快，个人在社会中无法脱离互联网的参与，我们不得不面对的问题就是在互联网空间个人应得的自由是什么。自由需要在安全和高效之间寻找平衡，毫无安全下的自由也不是真正的自由，个人权利下的自由往往和政府的监管之间是共生且相互补充发展的，是相互存在的概念，像一张纸的正反面，完全的自由不需要监管，可无监管安全的自由又不具有价值。诚然，在社会生活中，每个人都有权利决定自己当下的活动，可以选择自己的行为，自己的自由意志是被无条件支持的，但是涉及大数据技术的三方，脱离了政府监管的企业便会为了企业的利益通过数据推送、数据预测等多种方式潜移默化地影响你个人心中认为的自由选择，政府的参与监管是必需的，政府必须合理地控制企业这种影响个人倾向的行为，

但是政府又不能监管过度,监管过度又使个人的选择倾向无限地导向主流价值观倾向,个人的自我虽然能被引导到正确的方面,但又失去了自由,社会将失去创新创造能力,不能够具有活力。这就要求个人在互联网中既不能由于严密的监控或是数据预测的引导导致自由被禁锢,又说明了人只有在合理的规则和监督之下才能更好地谈自主、谈自由、谈自治。所以对于政府主体而言,为了让个人的隐私真正受到保护,我们需要构建自由与监管适度的伦理原则,在保障社会安全和个人安全的大前提下,公众适度的自由便是互联网时代隐私保护伦理原则的倾向点。评估好监管与自由二者之间的辩证关系,让政府监管企业和个人,在注重个人隐私的保护的同时,重视公众对个人自由的诉求。

3. 个人主体: 倡导自我负责的原则

构建从个体出发的伦理原则,便是自我对我隐私主动负责维护的出发点,主动自我采取方案,利用新知识、新方法,或者积极迎合政策等主动保护自我隐私。由于法律,技术维度发展的不全面,或者说尚且滞后,此时个人从伦理维度的角度来说必须发挥自己的主观能动性,并且执行才是最为直接的我隐私保护。在互联网空间里活动的每一个个人都是无法置身事外的,虽然企业或者是政府通过遵循了制度、制定了公约和升级相关技术等手段保护了个人的隐私,但个人必须积极迎合这些手段而且必须提高自我保护意识,尊重他人隐私,才是最直接的为我隐私负责的做法,只有每个人都树立和调整正确的隐私观念,在互联网空间内才能更好地作出保护自我隐私的行动,更好地配合政府的政策或是运用企业的隐私技术。正确的隐私观应该包含两个部分:一是明确自我隐私的边界,对于可能伤害自我隐私范围的行为及时避免,有意识地筛选互联网应用,对自我互联网上的社交行为或是购买行为进行有意识的防护,比如购物就要注意自我的真实信息,社交软件的动态不要涉及自己的敏感信息;二是自我隐私保护的责任意识,自我的责任意味着对个人隐私安全的重视,对隐私保护的重要性给予肯定。一旦意识到自我隐私受到侵犯或是侵害之时,尽快地通过法律手段或是其他手段来维护自己的隐私权利。虽然个体的力量比起组织的力量处于弱势的地位,但是个人的保护具有及时性和主动性。人们更应该注重自己的隐私,对自己隐私保护应具有高度的重视,明确范围,学习保护方法。互联网技术发展到今天,在隐私保护方面,法律法规依然缺乏完善系统的保护,提高并加强网民的自我角色意识和自我保护意识就变成了富有成效的方式方法。构建倡导自我为我隐私负责的伦理原则,不仅是一种自己对自己负责的美德,还能防范自身隐私的内部危

机。

(二) 进行大数据技术下的隐私保护的伦理道德教育

道德教育是一定社会的阶级依据一定的道德准则和要求,有组织有计划地对人们施加系统的道德影响的复杂过程^{[4](P28-29)}。这种有系统有要求有目标的教育过程有效地帮助了受教育者提高道德认知、陶冶道德情感、锻炼道德意志,随着主体自我道德意识的增强和道德行为的实践,有效地改善社会矛盾。因此,大数据技术下的伦理道德教育显得兼具效率和效果,对于诸多隐私保护伦理问题,教育下的个人不仅是素质要求下的结果,还是个人自己不断要求进步的结果。

大数据技术下的伦理道德教育应当注重两个方向:第一,正确的价值观培养。大数据技术对于市场而言,实实在在地带来利益与价值,但是相比人的尊严价值,我们需要作出正确价值观倾向。由于大数据技术本身的特性,会给人带来隐私风险,这种矛盾只能在统一中发展,即大数据带来的利益价值的风险与个人的尊严价值相平衡的价值观,既不能否定整个大数据技术,也要尊重个人隐私需要得到保障的权利。倡导经济的发展不能逾越个人的尊严人格,这是毋庸置疑的原则问题,不能舍远求近,要树立利益让步人格价值的正确价值观,完善对参与大数据技术各主体的价值观教育。第二,培养正确的责任伦理意识培养。责任伦理是一种将人作为唯一的责任主体的道德情感和内在责任感,强调人的道义担当和必须为自身行为后果负责的判断标准^{[5](P13-17)}。个人角色感在互联网空间中弱化,使得主体的责任感丧失,连带导致大数据技术下的伦理失范行为增加。在注重大数据技术发展的高效性的同时,政府应该加强责任伦理意识培养并起带头作用,建立系统的制度便于有效执行,起到道德价值定位的作用,让各主体不仅知道履行责任,还知道如何履行责任。

(三) 完善大数据技术下隐私保护的伦理道德约束机制

仅仅是通过伦理意识的教育是不够的,任何伦理问题的解决除了每个人自我的伦理意识,正确的道德观和价值观还需要具体的伦理道德约束的机制,将人本身与道德机制放在一起并行发展、相互促进。有了道德机制的约束,帮助了主体约束自身,有助于每个人更好地崇尚伦理道德并亲身实践。为了机制作用良好的运行,一是需要每个主体对伦理道德规范的认同;二是约束机制能够内化成主体自身的自觉行为;三是主体能够听到外部的声音,即发挥社会舆论监督和道德评价的功能,弥补自身不足和漏洞。

道德伦理约束机制可以从两点着手:一是完善隐私伦理保护的自律机制。自律是伦理道德中

的重要基本原则,每个人作为道德主体需要对自己的行为规范,履行相应的道德义务,这就代表着作为参与大数据技术下的各个主体都需要对自己的行为做到自觉履行道德义务,主体作为最能控制的自我,在数据生产中,更应当自觉地注意自身的隐私安全,提高自我的隐私保护意识并学习相应的隐私保护技能。为了去做成这件事,首先个人需要的是对自我隐私安全的重要性认知,要重视自我的隐私安全,这种做法就是从源头起到了防控。政府和各企业组织是下一层面的参与者,在信息搜集和数据使用分析上应该发挥好自身的主导和带头作用,因为是参与者,对于隐私的保护会需要更大的作为去引导隐私安全,尤其是政府,更需要起领导作用,规范自身并且引导好大数据技术的使用方式,约束企业自觉地规范自身道德行为,让全部的参与者认识到保护隐私安全是社会一致的公约,得到全社会的认同,每个主体就会有自觉的意识进行自律行为。二是强化社会舆论监督和道德评价功能。除了主体以外的社会监督和道德评价能够有效地让主体认识到自我自觉自律的不足之处,能够让不尽统一的道德观得到相互的借鉴和融合,所以强化社会舆论监督和道德评价是约束机制中的不可缺少的重要

一环。对于强化社会舆论监督的机制,政府可以建立多主体的监督体系,对大数据技术下的使用进行监控,从而起到预防的目的。多主体也意味着社会上大多数人的道德倾向,具有共同认识的价值较高,能引导道德伦理机制走向共同认同的方向,因此就具有更高的约束力和规范力。强化道德评价的功能,将道德评价致力于主体的自省,弥补主体原来道德认知的漏洞,既增强了主体遵守道德规范的主动性,也使人们将道德规范内化成自觉的行为。

[参 考 文 献]

- [1] 闫立,吴何奇. 重大疫情治理中人工智能的价值属性与隐私风险——兼谈隐私保护的刑法路径[J]. 南京师大学报: 社会科学版,2020(2).
- [2] 王军,蒋佳臻. 网络空间的隐私保护及治理研究[J]. 新闻爱好者,2019(7).
- [3] 王海明. 新伦理学[M]. 北京: 商务印书馆,2001.
- [4] 苏新民. 略论道德教育的系统性[J]. 学术界,1999(4).
- [5] 程立涛,崔秀荣. 论责任伦理的社会价值[J]. 石家庄学院学报,2007(4).

Big Data Value and Privacy Ethics Under The Epidemic Situation

YI Shu – fan

(School of Public Administration ,

Nanjing Normal University ,Nanjing 210046 ,China)

Abstract: The application of relevant big data technology provides an efficient and solid technical foundation for epidemic prevention and control. In the process of major epidemic control and prevention, big data technology provides high efficiency for epidemic prevention and control, reduces the loss of human resources, and makes the epidemic prevention and control more accurate. It is prepared to locate the population related to the epidemic situation, which not only improves the accuracy of diagnosis, but also provides medical personnel Members provide more information and prevention possibilities, and more ensure the safety of medical personnel. Big data can identify the degree of personal safety, such as the use of health codes, and also provide accuracy for screening under epidemic control, and provide efficiency for the subsequent economic recovery. However, the use principle of big data technology is the mining and use of personal data, and the invasion of personal privacy is unavoidable. The meaning of personal privacy is like a chameleon, which changes with the change of environment. Especially in China, the legal construction of the right to privacy is obviously insufficient. The right to privacy is not protected as a separate right, and it is always attached to various other rights, which makes the personal privacy crisis under big data more and more prominent. This paper attempts to supplement the protection of personal privacy from the perspective of ethics, and puts forward the specific path of personal privacy ethics construction under big data technology from the dialectical standpoint of epidemic prevention and control, social security and personal privacy.

Key words: epidemic prevention and control; big data technology; privacy crisis; privacy ethics

[责任编辑 薄 刚]